DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS BENEFITS ADMINISTRATION

Security and Access Controls for the Beneficiary Fiduciary Field System Need Improvement

AUDIT | REPORT #18-05258-193 | SEPTEMBER 12, 2019

The mission of the Office of Inspector General is to serve veterans and the public by conducting effective oversight of the programs and operations of the Department of Veterans Affairs through independent audits, inspections, reviews, and investigations.

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

The VA Office of Inspector General (OIG) conducted this audit to determine if the Beneficiary Fiduciary Field System (BFFS) had the necessary controls to protect data integrity and safeguard protected, personal fiduciary and beneficiary information. BFFS is the information technology system used to manage the caseload for VA's Fiduciary Program.

The Fiduciary Program manages payments for veterans and other beneficiaries who, due to injury, disease, or age, are unable to manage their financial affairs and are thus vulnerable to fraud or abuse.[1] In 2017, fiduciaries received about $3.1 billion in VA benefit payments on behalf of the more than 211,000 beneficiaries they serve.[2]

The Veterans Benefits Administration (VBA) deployed BFFS in May 2014 to replace the aging Fiduciary Beneficiary System and manage data on beneficiaries, including names, mailing addresses, social security numbers, medical record information, and financial information. BFFS stores information on fiduciaries appointed to manage veterans' finances, including their credit and criminal histories. This audit assessed system controls related to security management, user access, and the separation of duties within the system.

What the Audit Found

The OIG team found that VA's Office of Information and Technology (OIT) inappropriately set the security risk level for BFFS at moderate instead of high. This happened because risk managers did not follow established standards and did not consider the existence of protected health information (PHI) and personally identifiable information (PII) stored in the system's database. The lower security setting reduced the system's security and access controls and potentially jeopardized the confidentiality, integrity, and availability of sensitive information related to beneficiaries and fiduciaries. For example, a moderate risk system requires minimum security controls such as a response to audit processing failures and protection of audit information. A high-risk system maintains the same requirements as a moderate system but has additional controls including real-time alerts for responding to audit processing failures and backing up physical systems and components to protect audit information.

The OIG team also found that some system users could access records not needed to perform their duties. The Fiduciary Program operates from six geographical hubs. Each hub is assigned Pension and Fiduciary Service personnel who complete tasks related to their assigned

[1] A beneficiary is an individual entitled to receive VA benefits. Beneficiaries are classified as minors, veterans, and other adults. The latter group includes adult children incapable of self-support prior to their eighteenth birthday, surviving spouses, dependent parents, and some insurance payees.

[2] A fiduciary is a person or legal entity authorized by VA to serve as payee of VA benefits for a beneficiary unable to manage his or her financial affairs.

beneficiaries and fiduciaries. In some instances, a fiduciary and beneficiary may be in different geographic regions serviced by different hubs, creating the need for shared information between hubs. The OIG team found that more than 1,600 hub personnel have nationwide access to BFFS data. This is far beyond the number needed to address those limited instances in which information must be shared between hubs. Moreover, VBA does not have a process for reviewing these employees' access privileges. As a result, hub personnel can view records regardless of the physical location of beneficiaries and fiduciaries, which violates access requirements and increases the risk that beneficiary or fiduciary information could be misused.

VBA officials did not enable audit logs for all records and fields within BFFS out of concern that it would reduce the system's functionality. However, when combined with a user's ability to access records nationwide, this creates an unnecessary risk that unauthorized access to beneficiary PII, PHI, and other sensitive information will go undetected. Without fully functional audit logs, VBA cannot accurately and comprehensively track access to records, and fiduciary hub managers cannot effectively detect, report, and respond to security violations within BFFS. Therefore, fiduciary hubs are at an increased risk of being unable to detect personnel who inappropriately access, modify, or delete beneficiary records.

Finally, the OIG found that VBA did not ensure separation of duties were fully enforced during the field examination report submission process. For example, legal instrument examiners who are charged with approving reports submitted by field examiners could also edit the reports. This occurred because VBA did not require the field examiners to place a "cursory lock" on the reports so they could not be edited by others. Without a cursory lock, sensitive information within the field examiner report can be changed without approval or documentation.

What the OIG Recommended

The OIG made four recommendations to improve the BFFS security and access controls to protect data integrity and safeguard protected, personal fiduciary and beneficiary information. Recommendations include reevaluating the risk determination for BFFS, improving controls over end users' access levels, fully enabling audit logs to ensure VBA can accurately and comprehensively track access to records within BFFS, and improving separation of duties.

Management Comments

The principal deputy assistant secretary for information and technology and deputy chief information officer concurred with Recommendations 1−3. To address the recommendations, the principal deputy assistant secretary stated OIT will reevaluate the risk determination for BFFS to determine if the system should be set to a security categorization level of high based upon the PHI and other sensitive data maintained in the system. According to the principal deputy assistant secretary, the assessment will be completed by September 30, 2019. The principal deputy assistant secretary also stated BFFS should be migrating to Microsoft Dynamics 365

Azure Cloud by October 25, 2019, and the migration will provide activity logging features to track end-user activities, enable the creation of reports from audit logs, and provide managers the ability to generate a report to regularly review and monitor access levels to beneficiary and fiduciary records. In addition, the principal deputy assistant secretary stated OIT will coordinate with BFFS business partners to set the cursory lock as a default for data reports. According to the principal deputy assistant secretary, setting the cursory lock as a default in BFFS will require a custom code change that could be accomplished by February 12, 2020.

The under secretary for benefits concurred with Recommendations 1 and 4 and concurred in principle with Recommendation 2. Regarding Recommendation 1, the under secretary responded VBA will rely on OIT to reevaluate the risk determination for BFFS. In response to Recommendation 2, the under secretary stated VBA would rely on OIT to perform a risk assessment of access levels to beneficiary and fiduciary records. The under secretary also stated VBA will work in conjunction with OIT on the results of the risk assessment and subsequent compliance reviews. However, the under secretary expressed concerns about limiting employee access to systems based on geographic location because restricting access would limit workload management capabilities. In response to Recommendation 4, the under secretary stated VBA will create an interim procedure—while awaiting the required custom code change—to require field examiners to lock reports upon completion, which will prevent report overwriting by other users. Guidance on this procedure will be issued by September 30, 2019.

The principal deputy assistant secretary for information and technology and the under secretary for benefits submitted acceptable corrective action plans for the recommendations, including Recommendation 2, which the under secretary for benefits agreed to in principle. The OIG will monitor implementation of planned actions and will close the recommendations when VA provides sufficient evidence demonstrating progress in addressing the intent of the recommendations.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

BFFS	Beneficiary Fiduciary Field System
CRM	Customer Relationship Management
CRM/AF	Customer Relationship Management Application Framework
FISMA	Federal Information Security Management Act
OIG	Office of Inspector General
OIT	Office of Information and Technology
NIST	National Institute of Standards and Technology
PHI	protected health information
PII	personally identifiable information
VBA	Veterans Benefits Administration
VRM	Veterans Relationship Management

Introduction

The VA Office of Inspector General (OIG) conducted this audit to determine if the Beneficiary Fiduciary Field System (BFFS) had the necessary controls to protect data integrity and safeguard sensitive information. BFFS is the information technology system used to manage the caseload for VA's Fiduciary Program. Specifically, the audit assessed system controls related to security management, access, and separation of duties. The OIG made four recommendations for improvement related to three key findings.

Fiduciary Program

The Fiduciary Program manages payments for veterans and other beneficiaries who, due to injury, disease, or age, are unable to manage their financial affairs and are thus vulnerable to fraud or abuse.[3] The program operates from six hubs within the United States and its territories. The Veterans Benefits Administration (VBA) administers and provides oversight for its six hubs and the fiduciary and field examination activities at the VA regional office in Manila, Philippines.

Because these beneficiaries include VA's most vulnerable veterans, the Fiduciary Program ensures their protection and provides oversight of the fiduciaries who serve them. According to VA's 2019 congressional budget request, the Fiduciary Program experienced a 73 percent increase in the number of beneficiaries from about 122,000 in 2011 to over 211,000 in 2017; more than 50 percent of beneficiaries in the Fiduciary Program are age 80 or older.

Prior to a fiduciary's appointment, VBA conducts a field examination to ensure the physical and financial welfare of the beneficiary. Follow-up field examinations are conducted to assess the performance of the fiduciary and update beneficiary information.[4] The field examination results are compiled in a report that contains a significant amount of data such as a veteran's name, social security number, medical information, and financial account information. This data is used by legal instrument examiners to verify information contained in VBA's Corporate Database and to update BFFS.[5] According to VA's 2019 congressional budget request, fiduciary staff completed 89,000 field examinations in 2017, an 8 percent increase from 2016. In 2017,

[3] A beneficiary is an individual entitled to receive VA benefits. Beneficiaries are classified as minors, veterans, and other adults. The latter group includes adult children incapable of self-support prior to their 18th birthday, surviving spouses, dependent parents, and some insurance payees.

[4] A fiduciary is a person or legal entity authorized by VA to serve as payee of VA benefits for a beneficiary unable to manage his or her financial affairs.

[5] The Corporate Database is a highly normalized relational database, which is an integrated enterprise database that supports multiple VBA business lines and applications. The Corporate Database also promotes common data sharing among multiple benefit applications and maintains the veterans' data integrity on a single platform.

fiduciaries received about $3.1 billion in VA benefit payments on behalf of the more than 211,000 beneficiaries they serve.

Beneficiary Fiduciary Field System VBA deployed BFFS in May 2014 for fiduciary hub personnel to use in place of the aging Fiduciary Beneficiary System and to manage data on beneficiaries. BFFS is an electronic database that maintains beneficiary information, and, according to VA, provides more effective oversight of fiduciaries through improved reporting and monitoring of misuse. Furthermore, BFFS provides a case management product used for fiduciary oversight by quality and training specialists, legal instruments examiners, field examiners, fiduciary service representatives, fiduciary hub management personnel, and national VBA program analysts and management personnel. BFFS also provides real-time, robust and meaningful data capture to identify trends and conduct analyses, automatically and effectively assign fiduciary work through customized workflows, and track audits to improve user monitoring and data integrity.

Information Security Standards and Guidelines

The security controls in the National Institute of Standards and Technology (NIST) are designed to facilitate compliance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.[6] NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. This guideline is consistent with the requirements of the Office of Management and Budget Circular A-130, Section 8b (3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV, *Analysis of Key Sections*.

VA Handbook 6500 provides the risk-based process for VA information technology system security controls and operational requirements.[7] Specifically, the handbook requires that information systems have adequate audit logs, proper access privileges, and the appropriate system security categorization to protect data. The handbook also states that audit records and logs should document what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

[6] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

[7] VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,* March 2015.

The Federal Information Processing Standards Publication 199 establishes security categories for information types and information systems.[8] According to Publication 199, security categories are based on the potential organizational impact if certain events occur that jeopardize necessary information and systems. The security categorization for information type is based on the security objectives—confidentiality, integrity, and availability—within the system. The potential impact of each security objective could have a low (limited), moderate (serious), or high (severe or catastrophic) adverse effect on organizational operations, assets, or individuals.

Veterans Relationship Management and Customer Relations Management

The Veterans Relationship Management (VRM) and Customer Relationship Management (CRM) applications are two programs with a moderate security categorization that create a general support system. The VRM program currently hosts 12 moderate applications/systems, including BFFS, on the Customer Relationship Management Application Framework (CRM/AF) dedicated private cloud-hosted environment. According to VA's VRM CRM/AF Risk Assessment, dated September 19, 2018, the system environment received a Federal Information Security Management Act (FISMA) moderate authority to operate for systems with PII data and a FISMA high authority to operate for systems with protected health information (PHI) data.[9]

[8] According to the Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, information is categorized according to its information type, which is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, executive order, directive, policy, or regulation.

[9] Authority to operate is an accreditation decision authorizing a system to operate for an established amount of time (e.g., 30, 60, 90, 120 days) if certain conditions must still be met, or to operate and fall into the continuous monitoring process if all applicable security requirements have been met.

Results and Recommendations

Finding 1: BFFS Is Not Set at Appropriate Risk Categorization Level

VA's Office of Information and Technology (OIT) did not establish the appropriate risk security categorization level for BFFS, which reduced the system's security and access controls. For BFFS, the system risk security categorization level was set at a moderate level rather than high, which potentially jeopardized the confidentiality, integrity, and availability of beneficiaries' and fiduciaries' PHI, PII, or other sensitive information. This occurred because OIT did not adequately consider PHI as part of its BFFS risk assessment determination. In addition, VBA, the information owner and steward, did not participate in assessing the security categorization of BFFS as required by NIST.[10] This finding discusses security management related to BFFS risk categorization level. According to the Government Accountability Office's Federal Information System Controls Audit Manual, an entity-wide security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks.[11]

What the OIG Did

The OIG reviewed the VRM and CRM/AF risk assessment. The OIG also reviewed the account management policy, VRM CRM system security plan, and security controls assessments to determine if OIT identified and mitigated risk associated with the system. The OIG conducted interviews with OIT's deputy assistant secretary for the Enterprise Program Management Office and the director of information security risk management regarding the BFFS risk determination and authorization process. The OIG also interviewed OIT's information system security officer, privacy officer, information security officer, IT specialists, and the chief of Pension and Fiduciary Service at the time to assess security and access controls for BFFS.

BFFS Risk Security Categorization Level Set at Moderate

According to OIT's current director of information security risk management, he and the director at the time made the BFFS risk security categorization level determination under the VRM CRM/AF based on information contained in the Confidentiality, Integrity and Availability Classification questionnaire. The questionnaire, completed by an OIT contractor, assessed the

[10] NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* February 2010. The information owner or steward is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal.

[11] Federal Information System Controls Audit Manual provides a methodology for performing information systems control audits of federal entities in accordance with professional standards.

information type maintained in BFFS and indicated the system would not contain personal, private, or sensitive information. However, BFFS does contain this type of information.

NIST and VA Handbook 6500 determine the applicable security controls based on the risk level of the data in an information system.[12] Systems that contain PHI, such as BFFS, should be set at a risk security categorization level of high and include additional system controls. For example, a moderate risk system requires minimum security controls, such as a response to audit processing failures and protection of audit information. A high-risk system maintains the same requirements as a moderate system but also has additional controls including real-time alerts for responding to audit processing failures and backing up physical systems/components to protect audit information.

PHI Not Adequately Considered in System Risk Determination

OIT's information security officer, system owner, and system administrator, as well as VBA's privacy officer, did not adequately consider the extensive amount of PHI contained in BFFS when assessing the security categorization. The audit team evaluated OIT's Confidentiality, Integrity, and Availability Classification questionnaire and Privacy Impact Assessment used to assess the security categorization for BFFS. OIT used the questionnaire and assessment to determine the security and privacy controls needed to protect the types of information within BFFS. The questionnaire was inaccurate because the Privacy Impact Assessment indicated BFFS would collect a limited amount of PII to provide authorized individuals access to or interaction with VA.[13] Specifically, the assessment noted that BFFS would include names, mailing addresses, social security numbers, medical record information, and financial information. Also, BFFS would allow VA to maintain information on VA-appointed fiduciaries who manage veterans' finances, including their names, mailing addresses, social security or tax identification numbers, and credit and criminal histories.

The Federal Information Processing Standard Publication 199 establishes security categories for both information types and information systems. According to Publication 199, security categories are based on the potential organizational impact should certain events occur that jeopardize the information and systems needed. In addition, security categories should be used in conjunction with vulnerability and threat information in assessing risk. The Confidentiality, Integrity, and Availability Classification questionnaire and the Privacy Impact Assessment were used to assess the risk security categorization for BFFS. However, the information owner and

[12] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013.

[13] OIT and VBA staff interviewed did not provide justification for why the Confidentiality, Integrity, and Availability Classification questionnaire was inaccurate.

steward (VBA) did not participate in assessing the security categorization of BFFS as required by NIST.[14]

According to VA's Privacy Impact Assessment for BFFS, members of OIT's assessment team who participated in the risk determination included the system owner, the information security officer, the privacy officer, and the system administrator.[15] According to NIST, the information owners and stewards provide input to system owners regarding the security controls and security requirements for the systems. The audit team also found the VRM CRM/AF Risk Assessment did not identify information owners and stewards for the VRM applications hosted on the CRM/AF. VBA, including officials from Pension and Fiduciary Service, as the information owner and steward for BFFS, should have performed the categorization process in cooperation with OIT.

Because of the extensive amount of PHI, the audit team determined the system should be hosted in the FISMA high environment. This determination is consistent with the Federal Information Processing Standard Publication 199. Furthermore, the system environment for the VRM CRM/AF has a FISMA high authority to operate for systems that contain PHI data. For example, the Health Eligibility Center, Health Resource Center, and Veterans Crisis Line have applications/systems that have PHI data and are hosted on the FISMA high environment under CRM/AF.

Conclusion

Given the sensitivity of beneficiary information maintained in BFFS, the information is vulnerable to increased risks if there are insufficient system controls, and data compromise could potentially jeopardize the confidentiality, integrity, and availability of PII, PHI, and other sensitive information. The BFFS risk security categorization level should have been set at high to better protect both beneficiaries' and fiduciaries' information. In addition, OIT and VBA should have adequately considered PHI as part of the BFFS risk assessment determination. Furthermore, because BFFS contains PHI data, it should be hosted in the FISMA high environment.

Recommendation 1

1. The assistant secretary for information and technology, in conjunction with the under secretary for benefits, reevaluate the risk determination for the Beneficiary Fiduciary Field System and determine if the system should be set to a security categorization level

[14] NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* February 2010.

[15] Privacy Impact Assessments are conducted to identify privacy risks and identify methods to mitigate those risks to ensure that programs or information systems comply with legal, regulatory, and policy requirements and serve as notice to the public of privacy practices.

of high based upon the personal health information and other sensitive data maintained in the system.

Management Comments

The principal deputy assistant secretary for information and technology and deputy chief information officer concurred with the recommendation. In response to the recommendation, the principal deputy assistant secretary stated OIT will reevaluate the risk determination for BFFS to determine if the system should be set to a security categorization level of high based on the PHI and other sensitive data maintained in the system. According to the principal deputy assistant secretary, the assessment will be completed by September 30, 2019. The under secretary for benefits also concurred with the recommendation and will rely on OIT to reevaluate the risk determination for BFFS.

OIG Response

The principal deputy assistant secretary's corrective action plan is responsive to the intent of the recommendation. The OIG will monitor implementation of the planned action and will close the recommendation when VA provides sufficient evidence demonstrating progress in addressing the issue identified. The full text of the responses from the principal deputy assistant secretary and the under secretary for benefits is included in Appendix B.

Finding 2: BFFS Lacked Access Controls and System-Generated Audit Logs

The OIG found the lack of BFFS access controls allowed Pension and Fiduciary Service personnel (end users) to access records outside of their assigned fiduciary hub that were unnecessary to perform their duties.[16] End users are assigned to regionally-located offices called hubs, and primarily complete tasks related to assigned beneficiaries and fiduciaries in their geographic location. In limited instances, a fiduciary and beneficiary may be in different hubs, creating the need for shared hub responsibilities or dual jurisdiction. NIST and VA Handbook 6500 require user account management and the implementation of "least access privileges" to ensure that users are only accessing required records.[17] According to NIST, the principle of least privilege includes allowing access only for users that is necessary to accomplish assigned tasks consistent with their organizational missions and business functions. The OIG found that more than 1,600 hub end users have nationwide access to BFFS data. This is far beyond the number needed to address the limited number of cases in which more than one hub is implicated. Despite this disconnect, VBA does not have a process for reviewing access privileges.

As a result, end users can view records regardless of the physical location of beneficiaries and fiduciaries, which violates least access privileges and increases the risk that beneficiary information could be misused. In addition, BFFS does not generate audit logs to track end-user access to some records. Audit logs are enabled to record edits made to records and access to fiduciary records, but no audit logs were created to track end-user access to beneficiary records and field examination reports. When combined with the end users' ability to access records nationwide, this creates an unnecessary risk that unauthorized access to beneficiaries' PII, PHI, and other sensitive information will go undetected.

According to NIST and VA Handbook 6500 requirements, audit logs should be enough to track end-user access to records. According to the chief of Pension and Fiduciary Service at the time, officials decided not to enable audit logs for all records due to system performance concerns. The OIG team was unable to test whether limiting access controls or enabling audit logs would prevent necessary system performance or use. Having audit logs would enable VBA managers to monitor beneficiary data and track potential security breaches and internal information misuse. Without this control, fiduciary hub managers cannot determine if any unauthorized browsing or data theft is occurring within BFFS.

[16] Pension and Fiduciary Service personnel provide service to beneficiaries and oversight of VA-appointed fiduciaries.

[17] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

What the OIG Did

The OIG reviewed the account management policy, system security plan, and security controls assessments to determine if OIT identified and mitigated risk associated with BFFS. The OIG also interviewed OIT's information system security officer, privacy officer, information security officer, IT specialists, and the chief of Pension and Fiduciary Service at the time to assess security and access controls for BFFS. Finally, the OIG interviewed and observed hub end users such as field examiners, legal instrument examiners, fiduciary hub managers, and managers to determine their access within the system. The OIG also reviewed audit log capabilities within BFFS and assessed managers' abilities to determine what end users were accessing.

End Users Can Access Fiduciary and Beneficiary Data Nationwide

Fiduciary hub end users are assigned to a regionally-located hub and primarily oversee beneficiaries and fiduciaries located in those areas. However, the audit team found end users had access to beneficiary and fiduciary records regardless of the record location. The OIG determined that this level of nationwide access is not necessary to complete end users' responsibilities and violates the least access privilege principle while increasing the risk that beneficiary information is misused. Furthermore, the Federal Information System Controls Audit Manual, February 2009, notes that access controls provide reasonable assurance that access to computer resources is reasonable and restricted to authorized individuals.

According to the chief of Pension and Fiduciary Service at the time, BFFS was designed with usability rather than security in mind, which is why the system is set up to allow end users access to fiduciary and beneficiary records outside their fiduciary hub's area of responsibility. One benefit of this design is that end users can complete dual jurisdiction cases, where a beneficiary and a fiduciary are physically located in different hubs, without having to request additional access. However, an assistant hub manager stated that only about 25 percent of cases are dual jurisdiction. Based on this estimate, end users may need elevated privileges in limited situations, but generally should be restricted to accessing records in their own fiduciary hub.

The OIG team determined VBA should consider limitations on end-user access and assign a limited number of users with elevated privileges to process dual jurisdiction cases. Further compounding this issue, VBA does not have a process for reviewing access privileges with hub management. According to NIST, organizations are required to review accounts for compliance with requirements such as monitoring the use of information system accounts and authorizing access to the information system based on a valid access authorization and intended system use.

Audit Logs Did Not Track End-User Access to Beneficiary Records and Field Examiner Reports

Audit logs were not properly enabled to track end-user access. While it is important to track access to fiduciary records, access to beneficiaries' records should also be tracked because these include VA's most vulnerable veterans.

Although system functionality is important, an organization is required to provide adequate support for after-the-fact investigations of security incidents and to identify audit events that are significant and relevant to the security of information systems. According to NIST, audit records should include the necessary information to establish action taken by an end user, when and where it occurred, and the sources and outcomes of the action.[18] NIST also requires creating, protecting, and retaining audit records for monitoring, analyzing, investigating, and reporting unlawful, unauthorized, or inappropriate information system activity.

Without fully functional audit logs, VBA cannot accurately and comprehensively track access to records, and fiduciary hub managers cannot effectively detect, report, and respond to security violations within BFFS. Therefore, fiduciary hubs are at an increased risk of being unable to detect end users who inappropriately access, modify, or delete information within beneficiary records or field examiner reports. Tracking and reporting end-user access better protects beneficiaries from data theft due to unauthorized browsing.

The potential benefit of audit logs is exemplified in the case of a former field examiner who was convicted of defrauding a beneficiary in 2018. The former field examiner convinced a veteran to sign a will designating the examiner as the beneficiary of the veteran's estate. The fraud was only discovered after the former field examiner filed the will at a bank where the veteran had his accounts and the bank flagged it as suspicious. Although having audit logs would not have prevented fraud in this example, it is nearly impossible to determine if the former field examiner was viewing and stealing information from other beneficiary records. If audit logs were enabled, fiduciary hub managers could identify all records that the field examiner viewed to identify any other instances of potential fraud or data theft.

According to the chief of Pension and Fiduciary Service at the time, Pension and Fiduciary Service managers do not perform reviews of what records a user accesses or any changes they make to records. According to NIST, an organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity and reports findings to designated organizational officials. This includes auditing the results from monitoring account usage and configuration settings. The chief of Pension and Fiduciary Service at the time stated that if managers want to perform a review they must manually search records to determine if a

[18] Necessary information can include time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control.

change has been made, as there are currently no tools or reports that compile user changes. Having audit logs would help Pension and Fiduciary Service managers monitor beneficiary data and track potential security breaches or internal misuses of information.

Conclusion

The OIG determined end users should be restricted to accessing only required records in their own fiduciary hub. End users should only have access to those records necessary to accomplish assigned tasks consistent with organizational missions and business functions. Also, the lack of audit logs resulted in uncontrolled end-user access to sensitive data and contributed to limited program oversight that could mitigate the risk of unauthorized browsing and the subsequent misuse of information for personal gain. As the following recommendations indicate, OIT should work with VBA to review end-user access levels, as well as regularly evaluate access privileges to ensure appropriate access is assigned and audit logs are enabled to track end-user access.

Recommendations 2–3

2. The assistant secretary for information and technology, in conjunction with the under secretary for benefits, perform a risk assessment of access levels to beneficiary and fiduciary records, based upon the least privilege principle, and regularly review access to ensure that principle is enforced.

3. The assistant secretary for information and technology ensures audit logs within the Beneficiary Fiduciary Field System allow for management tracking of end-user access in order to reduce unauthorized browsing and the risk of data theft due to malicious activity.

Management Comments

The principal deputy assistant secretary for information and technology and deputy chief information officer concurred with Recommendations 2 and 3. In response to Recommendations 2 and 3, the principal deputy assistant secretary stated BFFS should be migrating to Microsoft Dynamics 365 Azure Cloud by October 25, 2019, and the migration will provide activity logging features to track end-user activities, enable the creation of reports from audit logs, and provide managers the ability to generate a report to regularly review and monitor access levels to beneficiary and fiduciary records.

The under secretary for benefits concurred in principle with Recommendation 2. In response to Recommendation 2, the under secretary stated VBA would rely on OIT to perform the risk assessment of access levels to beneficiary and fiduciary records. The under secretary also stated VBA will work in conjunction with OIT on the results of the risk assessment and subsequent compliance reviews. However, the under secretary expressed concerns about limiting employee

access to systems based on geographic location because restricting access would limit workload management capabilities.

OIG Response

The corrective action plans from the principal deputy assistant secretary for information and technology and the deputy chief information officer and the under secretary for benefits are responsive to the intent of the recommendations. The OIG will monitor implementation of planned actions and will close the recommendations when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the responses from the principal deputy assistant secretary and the under secretary for benefits is included in Appendix B.

Finding 3: Separation of Duties Was Not Fully Enforced

The OIG found VBA did not ensure separation of duties principles were fully enforced during the field examination report submission process. According to the Federal Information System Controls Audit Manual, segregation of duties provides reasonable assurance that duties are effectively segregated through formal operating procedures, supervision, and review. However, the OIG found legal instrument examiners who are charged with approving reports submitted by field examiners also could edit reports, which violates separation of duties controls.[19] This is because VBA did not require the field examiners to place a "cursory lock" on the reports so they could not be edited by others.[20]

These reports contain veterans' sensitive information such as social security numbers, medical information, financial account information, and their living conditions. NIST requires organizations to ensure separation of duties, as well as document controls and define information system access authorizations that support the separation of duties.[21] Requiring cursory locks is a necessary control to address the potential for abuse of authorized privileges and to help reduce the risk of malicious activity without collusion. Without a cursory lock, sensitive information within the field examiner report can be changed without approval or documentation.

What the OIG Did

The OIG reviewed the account management policy, VRM CRM system security plan, and security controls assessments to determine if OIT identified and mitigated risk associated with the system. The OIG also interviewed OIT's information system security officer, privacy officer, information security officer, IT specialists, and the chief of Pension and Fiduciary Service at the time to assess security and access controls for BFFS. Finally, the OIG interviewed and observed hub end users such as field examiners, legal instrument examiners, fiduciary hub managers, and other leaders to determine the access capabilities end users had within the system.

Field Examiner Reports Not Adequately Protected

Field examiners obtain a significant amount of information during their visits with beneficiaries, including their names, social security numbers, medical information, and financial account information. This information is compiled in a report and used by legal instrument examiners to verify and update the information in BFFS. It is also used to update the fiduciary information

[19] Legal instruments examiners share responsibility with supervisors, field examiners, and other fiduciary staff for making administrative and quasi-legal determinations involving the overall supervision of beneficiary estates and the protection of rights to benefits.

[20] Cursory locks are placed on field examination reports by a field examiner to prevent changes to the report.

[21] NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

directing the location of the beneficiary payments. When submitting these reports, field examiners have the capability to enable a cursory lock to protect the integrity of report data. Field examiner reports submitted without a cursory lock can subsequently be edited by a legal instrument examiner. The legal instrument examiner is responsible for accepting and approving the field examination report, and cursory locks are imperative to ensure no end user can unilaterally make changes within the report and then accept the changes made. Figure 1 shows a screen view of the cursory lock.

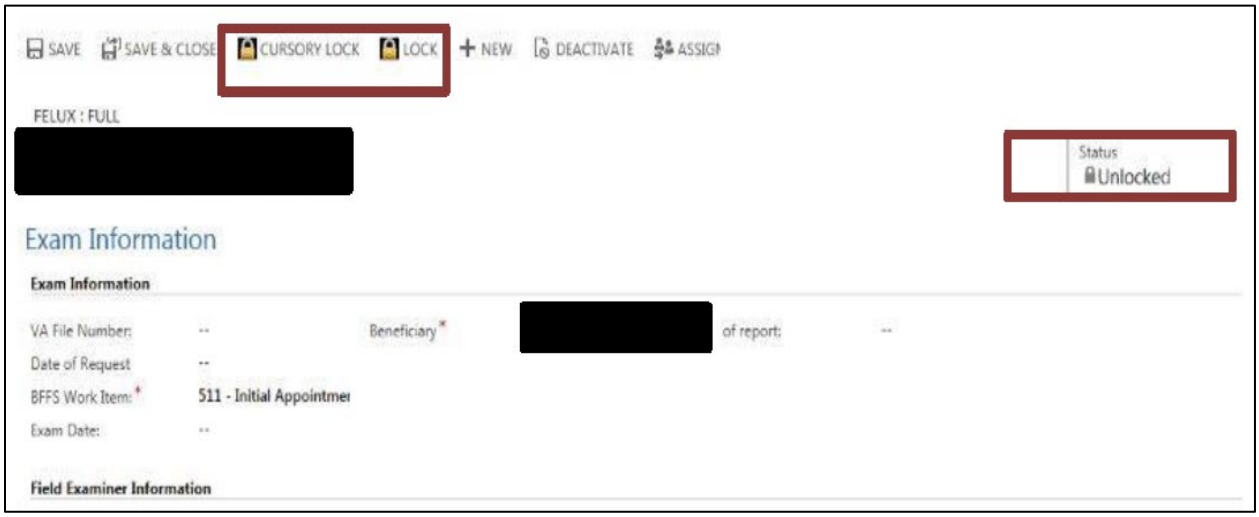

Figure 1. *BFFS record*
Source: BFFS screenshot provided by Pension and Fiduciary Service supervisory field examiner coach

According to the Fiduciary Program Guide, "once the [field examination report] is in cursory lock status, only the [field examiner] with ownership of the [report] is capable of unlocking the [field examination report]." A cursory lock prevents users other than the field examiner from making changes to the report, ensuring that the information contained within is protected. However, there is no requirement to submit a field examiner report with a cursory lock engaged. According to VA Handbook 6500, "access control software should be in place to limit individual authority and information access, whereby the collusion of two or more individuals is required to commit fraudulent activity." The handbook goes on to provide examples of separation of duties controls including supervisory review that a single individual does not perform combinations of functions, such as data entry, and verification of data or input of transactions that may result in a conflict of interest, fraud, or abuse.

The Fiduciary Program Guide also provides guidance for end users and specifically addresses cursory locks for field examination reports. The guide states a "cursory lock button allows the [field examiner] to lock all entities and sub-entities within [the field examination report]" and that "[field examiners] should utilize this function prior to submission of the [field examination report] to enhance data integrity" but does not make it a requirement. According to the chief of

Pension and Fiduciary Service at the time, field examiners were complaining that their work was being altered, therefore, the optional cursory lock control was added to BFFS.

Conclusion

Field examiner reports without the cursory lock engaged are at risk of having information within the report changed and approved by one person without any record. Consequently, inaccurate information could be used to update beneficiary and fiduciary files causing potential delays to beneficiaries' payments. Furthermore, not ensuring separation of duties principles were fully enforced created the potential for abuse of authorized privileges and the risk of malicious activity without collusion.

Recommendation 4

4. The under secretary for benefits ensures field examiners submit reports with a cursory lock engaged to protect their data integrity and to prevent separation of duties issues.

Management Comments

The under secretary for benefits concurred with the recommendation. In response to the recommendation, the under secretary stated VBA supports the use of the current BFFS functionality that allows field examiners to manually place a cursory lock on reports and will create an interim procedure to require field examiners to lock reports upon completion to preclude report overwriting by other users. The under secretary also stated VBA will issue the procedural guidance to the field examiners by September 30, 2019. In addition, the under secretary stated that the target date for setting the cursory lock as a default for data reports will be February 28, 2020.

The principal deputy assistant secretary for information and technology and deputy chief information officer also commented on the recommendation. The principal deputy assistant secretary stated OIT will coordinate with BFFS business partners to set the cursory lock as a default for data reports. According to the principal deputy assistant secretary, setting the cursory lock as a default in BFFS will require a custom code change that could be accomplished by February 12, 2020, during the next planned code change.

OIG Response

The under secretary for benefits' corrective action plan is responsive to the intent of the recommendation. The OIG will monitor implementation of planned actions and will close the recommendation when VA provides sufficient evidence demonstrating progress in addressing the issue identified. The full text of the responses from the under secretary and the principal deputy assistant secretary is included in Appendix B.

Appendix A: Scope and Methodology

Scope

The OIG performed this audit from July 2018 to July 2019 to determine if the defined roles for end users matched the system access roles, current information security controls were adequate, documentation existed for the process of granting access to BFFS, and any audit control processes were in place. In addition, the OIG evaluated whether the moderate risk security categorization level for BFFS was appropriate.

Methodology

The OIG reviewed the VRM CRM/AF risk assessment, account management policy, VRM CRM system security plan, and security controls assessments to determine if OIT identified and mitigated risk associated with the system. The OIG also interviewed OIT's deputy assistant secretary for the Enterprise Program Management Office and the director of information security risk management regarding the BFFS risk determination and authorization process. In addition, the OIG interviewed OIT's information system security officer, privacy officer, information security officer, IT specialists, and the chief of Pension and Fiduciary Service at the time to assess security and access controls for BFFS. VA security and access control policies were compared to NIST guidelines and standards. Configuration settings were compared to VA policies and procedures. The OIG also interviewed Pension and Fiduciary Service end users including field examiners, legal instrument examiners, coaches, and analysts at the Louisville, Kentucky, and Salt Lake City, Utah, fiduciary hubs to determine the access capabilities end users had within the system. Finally, the OIG reviewed audit log capabilities within BFFS and assessed managers' abilities to determine what information end users were accessing.

Fraud Assessment

The audit team assessed the risk that fraud, violations of legal and regulatory requirements, and abuse could occur during this audit. The audit team exercised due diligence in staying alert to any fraud indicators by soliciting the OIG's Office of Investigations for indicators. The OIG did not identify any instances of fraud or potential fraud during this audit.

Data Reliability

The audit team used computer processed data from the BFFS. To test the reliability of the data, the audit team determined whether users had access to BFFS, observed interactions with the system, and verified their name and email in the VA Active Directory. The audit team also assessed fiduciary data to test for key fields, obvious duplication of records, alphabetic or numeric characters in incorrect fields, or illogical relationships among data elements.

Furthermore, the audit team compared the beneficiary names, file number, social security number, and fiduciary contact information with VBA's Corporate Database and the Veterans Benefits Management System. The team determined that the data was sufficiently reliable for this audit's objectives.

Government Standards

The OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. The OIG believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objectives.

Appendix B: Management Comments

Department of Veterans Affairs Memorandum

Date: August 12, 2019

From: Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer (005A)

Subj: Draft Report, Audit of the Security and Access Controls for VA's Beneficiary Fiduciary Field System – Project No. 2018-05258-DV-0002

To: Assistant Inspector General for Audits and Evaluations (52)

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, Audit of the Security and Access Controls for VA's Beneficiary Fiduciary Field System (Project No. 2018-05258-DV-0002). The Office of Information and Technology (OIT) concurs with OIG's findings and recommendations and submits the attached written comments. For questions regarding OIT's comments on the draft report, please contact Martha Orr, Deputy Chief Information Officer for Quality, Performance, and Risk at (202) 461-5139.

(Original signed by)

Dominic Cussatt

Attachment

005 Attachment

Office of Information and Technology

Comments on OIG Draft Report,

Audit of the Security and Access Controls for VA's Beneficiary Fiduciary Field

System – Project No. 2018-05258-DV-0002

OIG Recommendation 1: OIG recommended the Assistant Secretary for Information and Technology, in conjunction with the Under Secretary for Benefits, reevaluate the risk determination for the Beneficiary Fiduciary Field System and determine if the system should be set to a security categorization level of high based upon the Personal Health Information and other sensitive data maintained in the system.

OIT Comments: Concur. The Office of Information and Technology (OIT) will reevaluate the risk determination for the Beneficiary Fiduciary Field System (BFFS) to determine if the system should be set to a security categorization level of high based upon the Personal or Protected Health Information (PHI) and other sensitive data maintained in the system. OIT will assess the amount of PHI in BFFS to ensure appropriate usage. OIT will complete said assessment by September 30, 2019 and provide the results to the Office of Inspector General.

OIG Recommendation 2: OIG recommended the Assistant Secretary for Information and Technology, in conjunction with the Under Secretary for Benefits, perform a risk assessment of access levels to beneficiary and fiduciary records, based upon the least privilege principle, and regularly review access to ensure that principle is enforced.

OIT Comments: Concur. The migration of BFFS to Microsoft Dynamics 365 Azure Cloud will provide activity logging features to track end user activities, such as “view,” “add,” “update,” and “delete”. Additionally, the migration will enable the creation of reports from audit logs. The upgrade provides management the ability to generate a report to regularly review and monitor access levels to beneficiary and fiduciary records. The BFFS Microsoft Dynamics 365 Azure Cloud migration is underway, with a kickoff meeting held on July 11, 2019. The target completion date for the migration is October 25, 2019. A high-level timeline is provided below:

Mobilize	06/24/2019 – 06/28/2019
Initiation	07/01/2019 – 07/12/2019
Build Phase	07/15/2019 – 09/09/2019
Stabilization	09/16/2019 – 10/04/2019
Deploy	10/07/2019 – 10/11/2019
Operate	10/14/2019 – 10/25-2019

OIG Recommendation 3: OIG recommended the Assistant Secretary for the Office of Information and Technology ensure audit logs within the Beneficiary Fiduciary Field System allow for management tracking of end user access, to reduce unauthorized browsing and the risk of data theft due to malicious activity.

OIT Comments: Concur. The migration of BFFS to Microsoft Dynamics 365 Azure Cloud will provide activity logging features to track end user activities, such as “view,” “add,” “update,” and “delete”. Additionally, the migration will enable the creation of reports from audit logs. The reporting feature will allow management to create reports to track end user access to reduce unauthorized browsing and the

risk of data theft due to malicious activity. The target completion date for the migration is October 25, 2019.

OIG Recommendation 4: OIG recommended the Under Secretary for Benefits ensure field examiners submit reports with a cursory lock engaged to protect their data integrity and to prevent separation of duties issues.

OIT Comments: Concur. BFFS functionality currently allows for field examiners to cursory lock reports to protect against modification or editing by other users. OIT defers to the Veterans Benefits Administration to implement a requirement for field examiners to lock reports.

As an additional measure, OIT will coordinate with BFFS business partners to set the cursory lock as a default for data reports. Setting the cursory lock as a default in BFFS will require a custom code change; there is currently a moratorium on BFFS code changes to support the Microsoft Dynamics 365 Azure Cloud Migration Project. The project is expected to be completed in October 2019, followed immediately by a transition phase. As a result, the next planned code change for a production release that could include setting the cursory lock as a default is estimated to be February 12, 2020.

Department of Veterans Affairs Memorandum

Date: August 15, 2019

From: Under Secretary for Benefits (20)

Subj: OIG Draft Report – Audit of the Security and Access Controls for the Beneficiary Fiduciary Field System Need Improvement [Project No. 2018-05258-DV-0002]

To: Assistant Inspector General for Audits and Evaluations (52)

Attached is VBA's response to the OIG Draft Report: Audit of the Security and Access Controls for the Beneficiary Fiduciary Field System Need Improvement.

Questions may be referred to Ruma Mitchum, Program Analyst, at (202) 632-8987.

(Original signed by)

Paul R. Lawrence, Ph.D.

Attachment

Attachment

Veterans Benefits Administration (VBA)

Comments on OIG Draft Report

Audit of the Security and Access Controls for the Beneficiary Fiduciary Field

System Need Improvement

VBA provides the following general comments:

VBA concurs with OIG's findings and recommendations in the draft report with one exception regarding the limitation of access for fiduciary hub employees as discussed in response to recommendation 2. Also, VBA is dependent upon the Office of Information and Technology to assist in addressing the risk determination, risk assessment, and in the development and implementation of system functionality to fully address OIG's recommendations.

The following comments are submitted in response to the recommendations in the OIG draft report:

Recommendation 1: The Assistant Secretary for Information and Technology, in conjunction with the Under Secretary for Benefits, reevaluate the risk determination for the Beneficiary Fiduciary Field System and determine if the system should be set to a security categorization level of high based upon the Personal Health Information and other sensitive data maintained in the system.

VBA Response: Concur. VBA defers to the Office of Information and Technology (OI&T) to reevaluate the risk determination for the Beneficiary Fiduciary Field System (BFFS).

Recommendation 2: The Assistant Secretary for Information and Technology, in conjunction with the Under Secretary for Benefits, perform a risk assessment of access levels to beneficiary and fiduciary records, based upon the least privilege principle, and regularly review access to ensure that principle is enforced.

VBA Response: Concur in principle. VBA defers to OI&T for the risk assessment of access levels to beneficiary and fiduciary records. VBA will work in conjunction with OI&T on the results of the risk assessment and subsequent compliance reviews. VBA cautions against limiting employee access to systems based on geographic location. While the fiduciary hubs are aligned via geographical boundaries, restricting access would greatly limit workload management capabilities. VBA does not limit access to systems for processing compensation or pension claims. The current practice is to allow nationwide access for claims processors in the Veterans Benefits Management System. As VBA continues to modernize its processing capabilities, the intent is to continue to have permission controls for employees, but to also move work electronically across the enterprise for efficiency.

Recommendation 3: The Assistant Secretary for the Office of Information and Technology ensure audit logs within the Beneficiary Fiduciary Field System allow for management tracking of end user access, to reduce unauthorized browsing and the risk of data theft due to malicious activity.

VBA Response: VBA defers to the Office of Information and Technology to develop the audit log functionality within BFFS.

Recommendation 4: The Under Secretary for Benefits ensure field examiners submit reports with a cursory lock engaged to protect their data integrity and to prevent separation of duties issues.

VBA Response: Concur. Current BFFS functionality allows field examiners to manually place a cursory lock on reports to protect against modification or editing by other users. VBA supports the utilization of this functionality and will create an interim procedure to require field examiners to lock reports upon

completion. This will preclude report overwriting by other users. VBA will issue the procedural guidance to the field examiners by September 30, 2019.

As an additional measure, OIT will coordinate with BFFS business partners to set the cursory lock as a default for data reports. However, setting the cursory lock as a default in BFFS will require a custom code change. Currently, there is a moratorium on BFFS code changes to support the Microsoft Dynamics 365 Azure Cloud Migration Project. The project is expected to be completed in October 2019, followed immediately by a transition phase. Therefore, the next planned code change for a production release that could include setting the cursory lock as a default is estimated to be February 12, 2020.

Target Completion Date: February 28, 2020

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Audit Team	Al Tate, Director Cynthia Christian Elijah Hancock Brandon Parrinello

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals
Additional Directors

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Reform
House Subcommittee on Technology Modernization
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

OIG reports are available at www.va.gov/oig.